IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
_____ Division

STRIKEFORCE TECHNOLOGIES, INC., **Plaintiff,** **v.** **SECUREAUTH CORPORATION,** **Defendant.**	Civil Action No. _____ **COMPLAINT FOR PATENT INFRINGEMENT** **JURY TRIAL DEMANDED**

COMPLAINT AND JURY DEMAND

StrikeForce Technologies, Inc. (hereinafter "Plaintiff" or "StrikeForce") files this Complaint for patent infringement against SecureAuth Corporation (hereinafter "Defendant" or "SecureAuth") for infringement of U.S. Patent Nos. 7,870,599; 8,484,698; and 8,713,701 (collectively, "Asserted Patents"). On personal knowledge as to Plaintiff's own actions, and on information and belief as to the actions of others, Plaintiff alleges as follows:

NATURE OF THE ACTION

1. This is a patent infringement action by StrikeForce to end SecureAuth's unauthorized and infringing manufacture, use, sale, offering for sale, and/or importation of products and methods in the U.S. incorporating StrikeForce's patented inventions.

2. Plaintiff StrikeForce seeks monetary damages, pre-judgment and post-judgment interest, and injunctive relief for SecureAuth's past and on-going infringement of the Asserted Patents.

THE PARTIES

3. Plaintiff StrikeForce Technologies, Inc. is a corporation organized and existing under the laws of the State of Wyoming, having its principal place of business located at 1090 King Georges Post Road, Edison, NJ 08837.

4. Upon information and belief, defendant SecureAuth Corporation is a corporation organized under the laws of the State of Delaware, having its principal place of business located at 8845 Irvine Center Drive, Irvine, CA 92618, and with its East Region Mid Atlantic Office located at 11710 Plaza America Drive, Suite 20, Reston, VA 20190.

JURISDICTION AND VENUE

5. This is a civil action for patent infringement arising under the patent laws of the United States, Title 35, United States Code §§ 1, *et seq.*

6. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

7. This Court has personal jurisdiction over SecureAuth because, upon information and belief, SecureAuth maintains continuous and systematic contacts and directs its activities at residents of, and has committed acts of infringement in, the Commonwealth of Virginia, including in this District. For example, upon information and belief SecureAuth maintains an interactive website, https://www.secureauth.com/, available to residents of the Commonwealth of Virginia, including residents in this District, wherein users of the website can purchase and/or request SecureAuth products, including its infringing "SecureAuth IdP" and "SecureAuth Cloud Access" products. Upon information and belief, SecureAuth also makes available mobile applications available for download to residents of the Commonwealth of Virginia, including residents in this District, including SecureAuth's "SecureAuth Authenticate" application.

8. In addition, upon information and belief, SecureAuth maintains continuous and systematic contacts, and has a regular and established place of business, through its East Region Mid Atlantic Office, located at 11710 Plaza America Drive, Suite 20, Reston, VA 20190. *See* https://www.secureauth.com/contact (last visited Mar. 15, 2017).

9. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(a)-(c) and 1400(b).

STRIKEFORCE OUT-OF-BAND PATENTS AND PRODUCTS

10. U.S. Patent No. 7,870,599 (the "'599 patent"), titled "Multichannel Device Utilizing a Centralized Out-of-Band Authentication System (COBAS)," was duly and legally issued on January 11, 2011. StrikeForce Technologies, Inc. is the owner by assignment of all right, title, and interest in and to the '599 patent, including without limitation the right to sue and recover for past, current, and future infringement thereof. A copy of the '599 patent is attached as Exhibit A to this Complaint.

11. U.S. Patent No. 8,484,698 (the "'698 patent"), titled "Multichannel Device Utilizing a Centralized Out-of-Band Authentication System (COBAS)," was duly and legally issued on July 9, 2013. The '698 patent is a continuation of, and claims priority to, the '599 patent. StrikeForce Technologies, Inc. is the owner by assignment of all right, title, and interest in and to the '698 patent, including without limitation the right to sue and recover for past, current, and future infringement thereof. A copy of the '698 patent is attached as Exhibit B to this Complaint.

12. U.S. Patent No. 8,713,701 (the "'701 patent"), titled "Multichannel Device Utilizing a Centralized Out-of-Band Authentication System (COBAS)," was duly and legally issued on April 29, 2014. The '701 patent is a continuation of, and claims priority to, the '599 and '698 patents. StrikeForce Technologies, Inc. is the owner by assignment of all right, title,

and interest in and to the '701 patent, including without limitation the right to sue and recover for past, current, and future infringement thereof. A copy of the '701 patent is attached as Exhibit C to this Complaint.

13. The inventions of the '599, '698, and '701 patents are directed to multichannel security systems and methods for authenticating a user seeking to gain access to, for example, Internet websites and VPN networks, such as those used for conducting banking, social networking, business activities, and other online services. This field of technology relates to what is sometimes referred to as "out-of-band" authentication or a type of "two-factor" or "multi-factor" authentication.

14. StrikeForce offers a product called ProtectID® that performs out-of-band authentication according to the teachings of one or more of the Asserted Patents. StrikeForce has offered this product since August 2003, and ProtectID® has displayed the statutory patent notice for its issued patents at its website, www.strikeforcetech.com, since about February 2011. In particular, StrikeForce's website identified the '599 patent at least as early as February 2011; StrikeForce's website identified the '698 patent at least as early as October 2013; and StrikeForce's website identified the '701 patent at least as early as June 2014.

15. Upon information and belief, SecureAuth has had actual knowledge of the '599 patent, '698 patent, and the '701 patent at least as early as, and no later than, the filing of this Complaint.

SECUREAUTH'S INFRINGING PRODUCTS

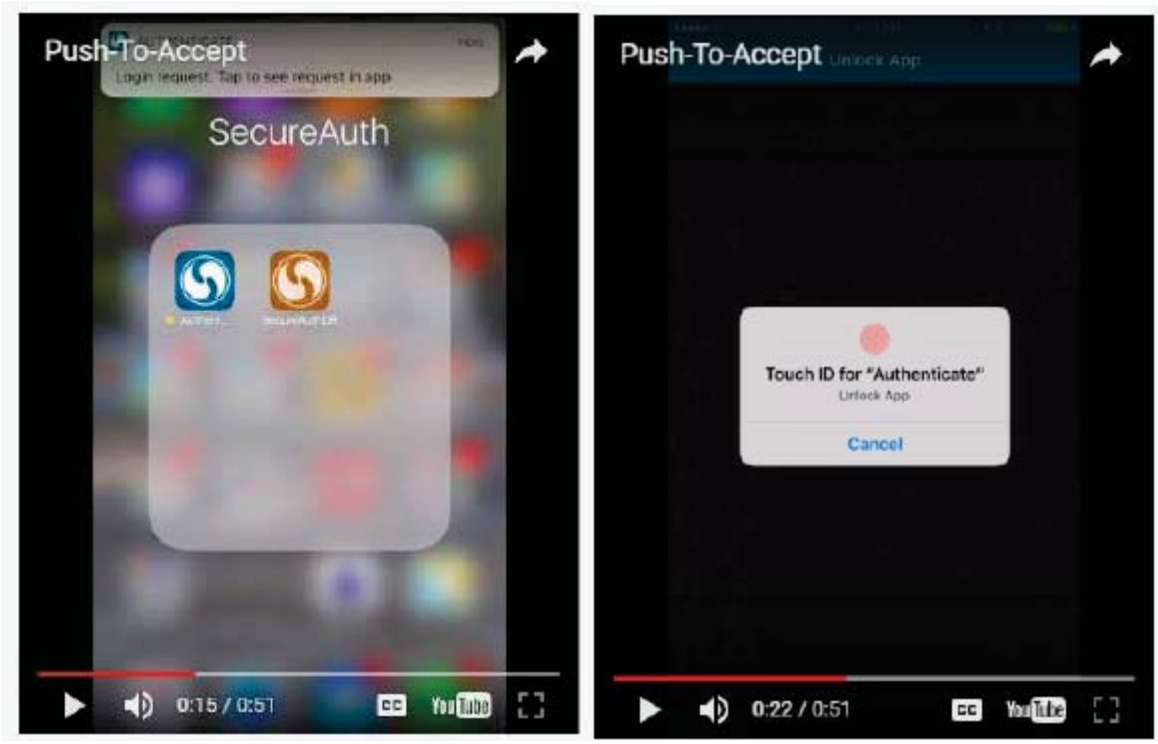
16. Upon information and belief, SecureAuth offers two-factor authentication products for use on Android and/or iOS devices in the United States and in this District. These products include, but are not limited to, SecureAuth IdP and SecureAuth Cloud Access

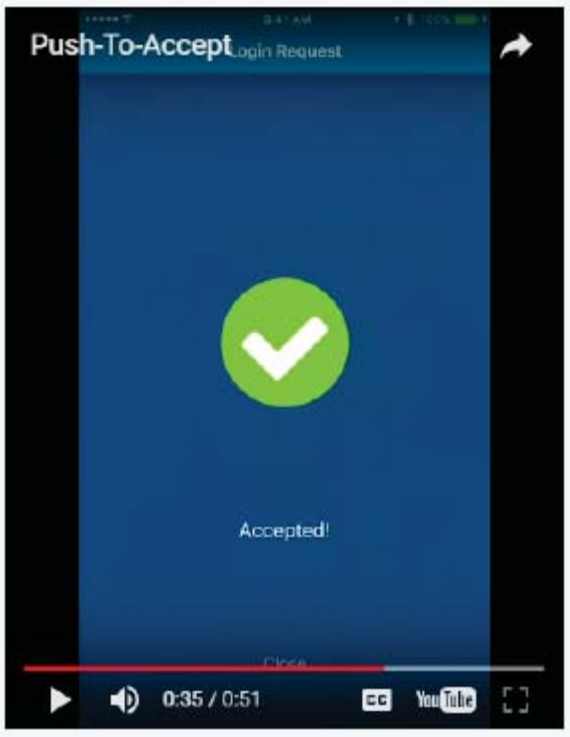
(collectively, "SecureAuth Products"). *See, e.g.*, https://www.secureauth.com/products (last visited Mar. 15, 2017).

17. Upon information and belief, SecureAuth Products utilize out-of-band technology that sends a notification to a user's device (*e.g.*, through the SecureAuth Authenticate mobile application) when a login request is made to provide out-of-band, two-factor authentication with a user's mobile device, such as a smartphone. According to SecureAuth, it offers "25+ Authentication Methods" as part of its "Multi-Factor Authentication" functionalities, including, among others, out-of-band two-factor authentication features referred to as "Push-to-Accept" and "Symbol-to-Accept" (*see* Exhibit K):

18. With respect to "Push-to-Accept," as SecureAuth explains on its website, available at https://www.secureauth.com/resources/blog/mobile-based-authentication (last visited Mar. 15, 2017), "Take your typical Push-to-Accept solution…. As a form of two-factor protection…. [the users] log into a protected resource with their username and password, and a notification is sent to their phone. If it's legitimate, the user hits the 'Accept' button. If it's not, the user hits 'Deny'…." An exemplary demonstration of this process for Push-to-Accept

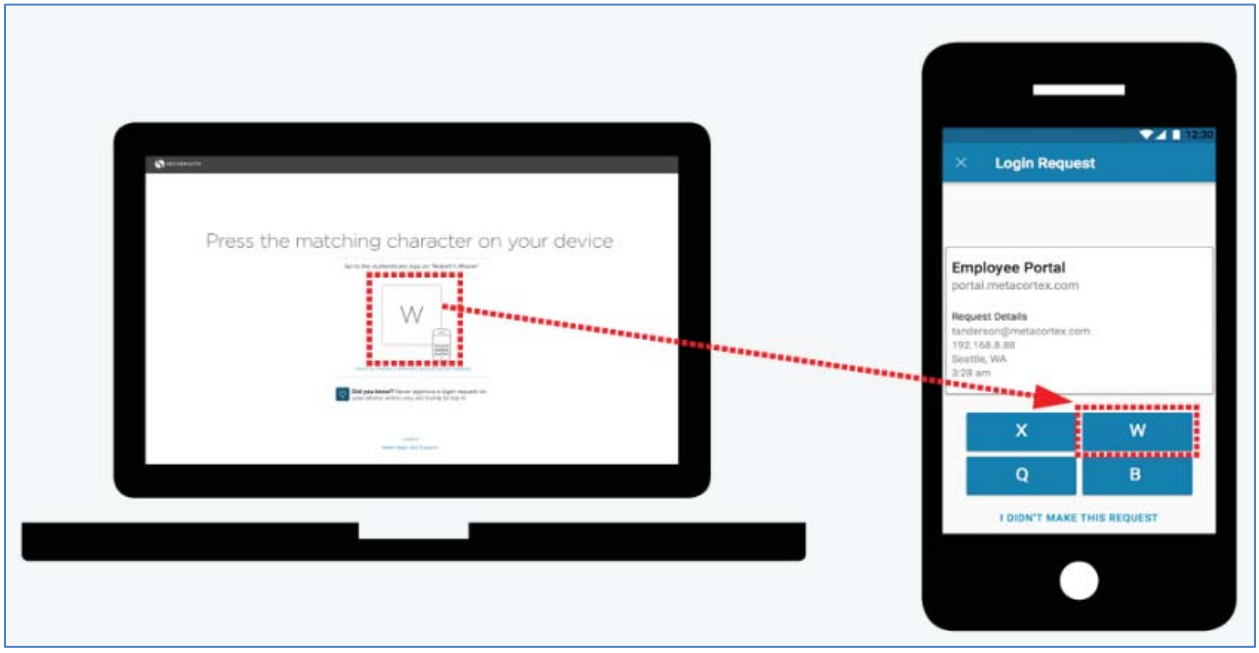
functionality using the SecureAuth Authenticate mobile application is shown on a video on SecureAuth's website, in Exhibit L, available at https://www.secureauth.com/solutions/industry-solutions/healthcare (last visited Mar. 15, 2017), screenshots from which are reproduced below:





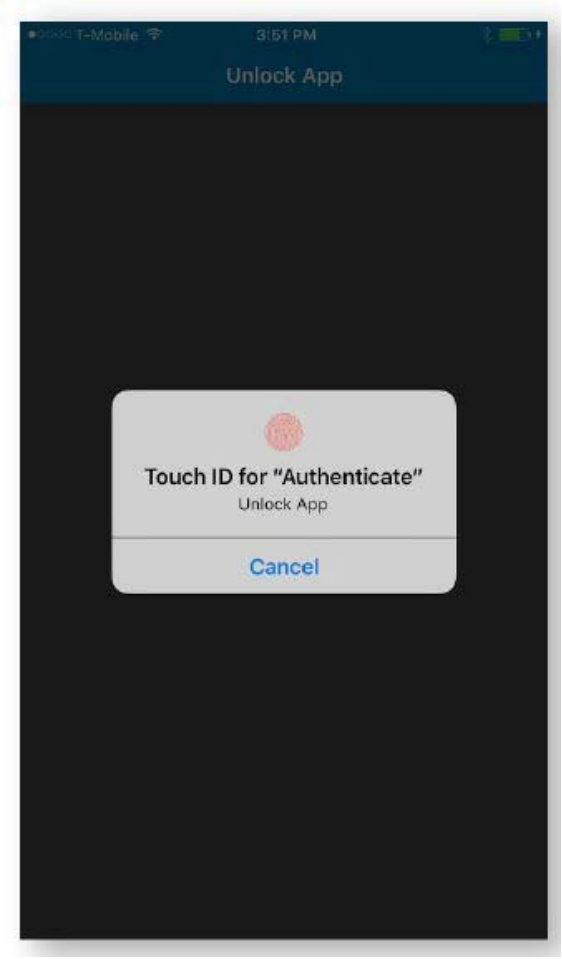
19. Upon information and belief, with respect to "Symbol-to-Accept," which is a type of push-to-accept functionality, SecureAuth explains on its website, available at https://www.secureauth.com/resources/blog/mobile-based-authentication (last visited Mar. 15, 2017), "With Symbol-to-Accept, the user … [is] not merely asked to hit an 'Accept' or 'Deny' button. Instead they're asked to validate their identity by selecting a symbol or letter on their mobile device that matches the one shown on their browser." An exemplary illustration of the

symbol-to-accept feature is reproduced below (*see* Exhibit N):



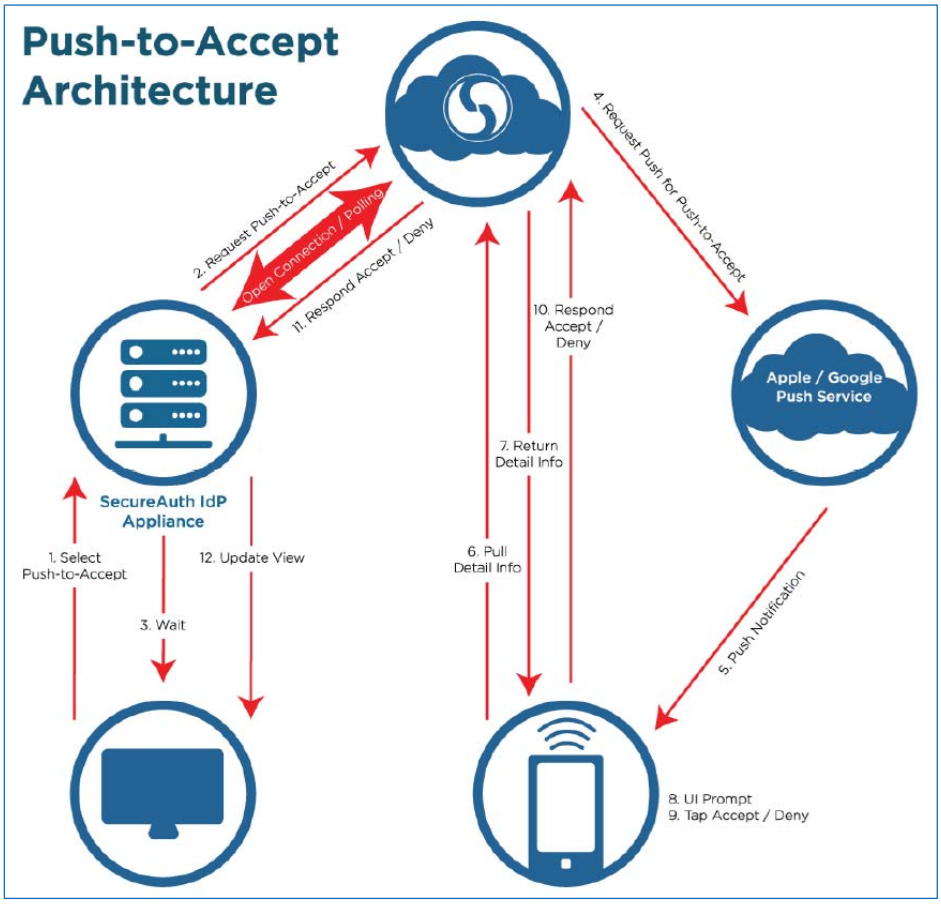
20. Upon information and belief, SecureAuth IdP comprises a system and/or service that incorporates a server (or servers) (*e.g.*, "SecureAuth IdP Server") for receiving and authenticating requests for access (*e.g.*, through a login attempt) to protected information residing on a computer (or computers), including through website applications, incorporating SecureAuth's Multi-Factor Authentication functionalities. SecureAuth IdP can additionally incorporate a RADIUS server (or servers) for receiving and authenticating requests for access to computers, including web applications. *See*, *e.g.*, Exhibit E; Exhibit F. When a user uses a device, such as a computing device, to attempt to access the protected computer or application, such as through the Internet, the user's request for access is directed to the SecureAuth IdP Server. The SecureAuth IdP Server retrieves information about the user from a database, such as a phone number or address of the user's mobile device, and sends a "push" notification out-of-band to the user's mobile device, requesting authorization for the access request.

21. Upon information and belief, when the push notification arrives on the user's mobile device, the user is prompted to open a previously downloaded SecureAuth mobile application to see the details of the authorization request. The user may be asked to input biometric data, *e.g.*, by scanning his or her fingerprint in order to open the SecureAuth mobile application (*e.g.* SecureAuth Authenticate) as an additional layer of authentication. An exemplary screenshot of this feature, available at https://itunes.apple.com/us/app/secureauth-authenticate/id615536686?mt=8 (last visited Mar. 15, 2017), *see* Exhibit H, is reproduced below:



22. Upon information and belief, the user is then prompted to respond to the login request by transmitting a response using SecureAuth's mobile application running on the user's mobile device to either accept or deny the request. The user may be presented with a Push-to-

Accept choice to select either an "Accept" or "Deny" response or may instead be prompted to select one out of several symbols that corresponds to a symbol displayed to the user on the device with which the request for access was made. The user's response is delivered to the SecureAuth IdP Server through an out-of-band channel. Once the user's response is validated by the SecureAuth IdP Server, the requested access to the protected computer or application will be granted. *See, e.g.*, Exhibit E, Exhibit G; Exhibit I; Exhibit J; Exhibit K; Exhibit L; Exhibit M; Exhibit N; Exhibit O; Exhibit P. An exemplary diagram of the Push-to-Accept system architecture, in Exhibit G at 2, is reproduced below:



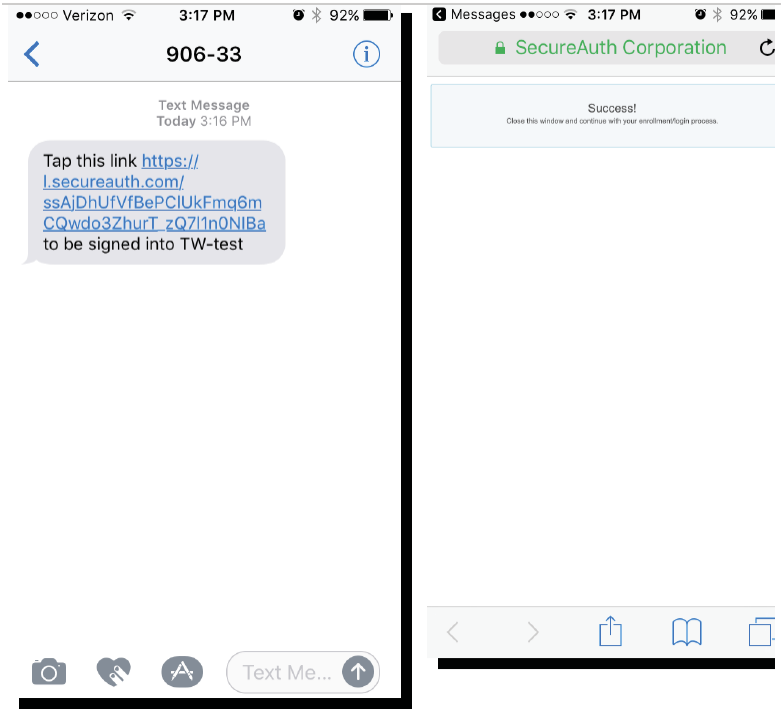
23. SecureAuth explains that these features "provide[] stronger authentication and greater confidence than passwords," in Exhibit I, available at https://www.secureauth.com/sites/default/files/sa_ds_idp.pdf:

24. Upon information and belief, SecureAuth Cloud Access ("Cloud Access") similarly utilizes out-of-band technology in the "cloud" (*i.e.*, over the Internet) that sends a notification to the user's mobile device when a login request is made to provide two-factor authentication with, *e.g.*, a mobile phone, incorporating SecureAuth's Multi-Factor Authentication functionalities. Cloud Access is designed to integrate with SecureAuth's clients' existing network and protected computers and applications to provide a cloud-based authentication service. Upon information and belief, Cloud Access utilizes out-of-band mobile push authentication sent from a server ("Cloud Access Server") to authorize a user's login request —*e.g.*, using SecureAuth's "Push-to-Accept" and/or "Symbol-to-Accept" features—prior to granting access to a protected computer or application in the same or a similar way as SecureAuth IdP. *See, e.g.*, Exhibit O; Exhibit M; Exhibit Q.

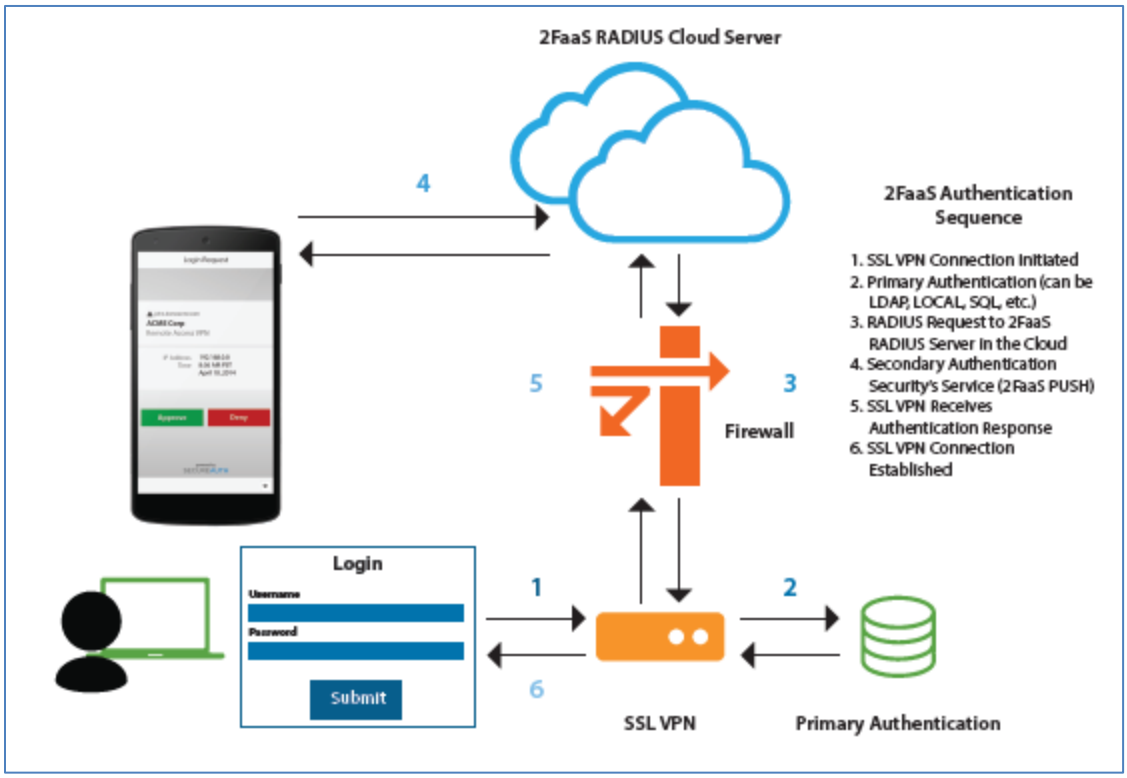
25. In one of SecureAuth's Cloud Access demonstration videos, available at https://www.secureauth.com/products/cloud-access/demos (last visited Mar. 15, 2017) and https://www.youtube.com/watch?v=o0DiUZpRbcY (last visited Mar. 15, 2017), SecureAuth explains, "[i]f I come in here into the security interface, I've got a multi-factor authentication

capability. So… this first screen is just showing what our authentication methods are. At launch, we got a variety of methods through the SecureAuth Authenticate app… so we can handle push notifications … where the user just has… to swipe and say accept." An exemplary screenshot from this demonstration, indicating the Cloud Access Push-to-Accept capability, is reproduced in Exhibit M (box checked for "Push Notification: Accept/Deny Login Request"); *see also* Exhibit P ("SecureAuth's Multi-Factor Authentication secures user's access into the Cloud Access Portal …. Users can employ SecureAuth's Authenticate App (iOS and Android) to … deliver … Push-to-Accept login requests ….").

26. Upon information and belief, Cloud Access also utilizes out-of-band mobile SMS "one-time link" technology sent from the Cloud Access server to authorize a user's login—*e.g.*, by sending a text message to the user's mobile phone containing a link, wherein the user "clicks [the] link, and then is permitted access." *See, e.g.*, Exhibit P at 1, 5-7.



27. Upon information and belief, a SecureAuth white paper entitled "SecureAuth 2-Factor as a Service 2FaaS," in Exhibit O, available at http://innetworktech.com/wp-content/uploads/2013/11/SECUREAUTH-2-FACTOR-AS-A-SERVICE-2FaaS.pdf (last visited Mar. 15, 2017), describes the structure of (or a structure similar to) SecureAuth's Cloud Service system. An exemplary diagram of the system structure, in Exhibit O, is reproduced below:



COUNT I –INFRINGEMENT OF THE '599 PATENT

28. StrikeForce incorporates by reference the averments set forth in paragraphs 1 through 27.

29. Pursuant to 35 U.S.C. § 271(a), SecureAuth has directly infringed and continues to directly infringe the '599 patent by making, using, selling, offering for sale, and/or importing in the United States products, software, and/or services that incorporate or make use of one or more of the inventions covered by the '599 patent, including, but not limited to, systems,

services, and/or software incorporating or implementing SecureAuth IdP and SecureAuth Cloud Access, including mobile applications working in conjunction therewith such as SecureAuth's Authenticate application (collectively, the "Accused Products"). SecureAuth thereby directly infringes one or more claims of the '599 patent, including at least claim 1 of the '599 patent. SecureAuth directly infringes at least through its own activities in making, using (including through testing), selling, offering for sale, and/or importing the Accused Products as well as, to the extent applicable, jointly with activities of others under the direction and control of SecureAuth, including customers of SecureAuth and/or distributors who sell and offer to sell the Accused Products.

30. Upon information and belief, and as demonstrated by the allegations above and the supporting exhibits to this Complaint, the Accused Products satisfy each and every element of one or more claims of the '599 patent, including, and without limitation, at least claim 1 of the '599 patent.

31. For example, and without limitation, the Accused Products comprise a multichannel security system for accessing a host computer (*e.g.*, software-based authentication platform of SecureAuth IdP and Cloud Access). *See, e.g.*, Exhibit D at 1; Exhibit E at 1–5; Exhibit G at 1–2; Exhibit H at 1; Exhibit I at 1–2; Exhibit J at 7, 9; Exhibit K at 1–2; Exhibit L at 1–5; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 2–6, 8, 10–12; Exhibit P at 1–3, 5–7; Exhibit Q at 1–2. The Accused Products include an access channel comprising interception means for receiving and verifying a login identification originating from a demand from an accessor for access to said host computer (*e.g.*, an element of the system that intercepts the user's login request and verifies the login information of the user prior to granting access to the protected information in, for example, the computer or application). *See, e.g.*,

Exhibit E at 1–5; Exhibit F at 2–3; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2; Exhibit N at 1–2; Exhibit O at 4–6, 8. The Accused Products include an authentication channel comprising a security computer (*e.g.*, SecureAuth IdP Server or Cloud Access Server) for receiving from said interception means said demand for access together with said login identification and for communicating access information to said host computer and for communicating with a peripheral device of said accessor (*e.g.*, push notification to user's mobile device requesting user to select, for example, a symbol). *See, e.g.*, Exhibit E at 4-5; Exhibit F at 1; Exhibit G at 1–2; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2; Exhibit N at 1–2; Exhibit O at 4–6, 8; Exhibit P at 6–7. The Accused Products include a database having at least one peripheral address record corresponding to said login identification (*e.g.*, database accessed by SecureAuth IdP Server or Cloud Access Server for communicating with the user's mobile device). *See, e.g.*, Exhibit H at 2–3 (explaining how a user enrolls the SecureAuth Authenticate mobile app into the SecureAuth IdP system); *see also, e.g.*, Exhibit I at 2; Exhibit L at 1–2; Exhibit N at 1–2; Exhibit O at 4–6. The Accused Products include prompt means for instructing said accessor to re-enter predetermined data at and retransmit predetermined data from said peripheral device (*e.g.*, an element of the system that issues a push notification on the user's mobile device prompting the user to select a symbol). *See, e.g.*, Exhibit F at 22–23; Exhibit G at 1–2; Exhibit H at 9–11; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2, 4; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 4–6, 8; Exhibit P at 7. The Accused Products include comparator means for authenticating access demands in response to the retransmission of said predetermined data by verifying a match between said predetermined data and said re-entered and retransmitted data, wherein said security computer outputs an instruction to the host computer to either grant access thereto

using said access channel or to deny access thereto (*e.g.*, SecureAuth IdP Server or Cloud Access Server receives the user's response and outputs an instruction to the protected computer to grant or deny access to the requested protected computer or application based on that response). *See, e.g.*, Exhibit E at 4; Exhibit G at 1–2; Exhibit H at 9; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 4–5; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 4–6, 8, 10–12; Exhibit P at 7.

32. Under 35 U.S.C. § 271(b), SecureAuth has indirectly infringed and continues to indirectly infringe the '599 patent by, *inter alia*, inducing others to make, use, sell, offer for sale, and/or import into the United States the Accused Products. SecureAuth distributes, markets, and/or advertises the Accused Products in this District and elsewhere in the United States, including through at least SecureAuth's website and online demonstrations of its products. *See, e.g.*, Exhibits D–Q.

33. Upon information and belief, with knowledge of the '599 patent and its infringement thereof, SecureAuth distributes its marketing materials and advertisements, and provides support for installing and implementing the Accused Products, to knowingly instruct and direct users/customers to use the Accused Products in an infringing manner.

34. Under 35 U.S.C. § 271(c), with knowledge of the '599 patent and its infringement thereof, SecureAuth has indirectly infringed, and continues to indirectly infringe the '599 patent by, *inter alia*, knowingly providing to its customers the Accused Products, which constitute material components of an infringing out-of-band authentication system/service and that was especially made or adapted for use in that system, which are not staple articles or commodities of commerce and which have no substantial, non-infringing use. *See, e.g.*, Exhibit D at 1; Exhibit E at 1–5; Exhibit F at 1–26; Exhibit G at 1–2; Exhibit H at 1–13; Exhibit I at 1–2; Exhibit J at 9;

Exhibit K at 1–2; Exhibit L at 1–5; Exhibit M at 1Exhibit N at 1–2; Exhibit O at 4–6, 8, 10–12; Exhibit P at 1–7.

35. SecureAuth puts the Accused Products into service and exercises control over said systems.

36. SecureAuth had and/or has knowledge of the ’599 patent and its infringement thereof at least as early as the filing of this Complaint.

37. SecureAuth’s customers directly infringe one or more claims of the ’599 patent by, for example, integrating the claimed systems and methods, including at least claim 1, directly into the customers’ web services and/or existing protected access control systems and directly benefitting from the use of those services and/or systems. For example, SecureAuth’s customers in the United States utilize the two-factor authentication systems and methods claimed in the ’599 patent, including at least claim 1, for the purpose of gaining secure access to, exemplarily, various Internet websites and other secure networks.

38. Upon information and belief, SecureAuth knowingly provides its customers with products and web services that are used in a manner that infringes one or more claims of the ’599 patent, including at least claim 1, as illustrated exemplarily above in paragraph 31.

39. Upon information and belief, through its marketing activities, instructions and directions, and through the sales and offers for sale of infringing systems and methods, SecureAuth specifically intends for, and/or specifically encourages and instructs, its customers to use its products and web services and knows that its customers are using its products and web services in an infringing manner.

40. As a direct and proximate result of SecureAuth’s acts of infringing one or more claims of the ’599 patent, StrikeForce has suffered injury and monetary damages for which

StrikeForce is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for SecureAuth's infringement.

41. SecureAuth will continue to directly infringe one or more claims of the '599 patent, causing immediate and irreparable harm to StrikeForce unless this Court enjoins and restrains SecureAuth's activities, specifically the acts of making, using, selling, and offering for sale, as previously outlined. There are inadequate remedies available at law to compensate for this harm.

42. Upon information and belief, SecureAuth's past and ongoing infringement of the '599 patent has been and continues to be with full knowledge of the '599 patent and SecureAuth's infringement thereof, at least as of the filing date of this Complaint. SecureAuth's knowing, willful, and deliberate infringement of one or more claims of the '599 patent, including at least claim 1, in conscious disregard of StrikeForce's rights makes this case exceptional within the meaning of 35 U.S.C. § 285 and justifies treble damages pursuant to 35 U.S.C. § 284.

COUNT II –INFRINGEMENT OF THE '698 PATENT

43. StrikeForce incorporates by reference the averments set forth in paragraphs 1 through 42.

44. Pursuant to 35 U.S.C. § 271(a), SecureAuth has directly infringed and continues to directly infringe the '698 patent by making, using, selling, offering for sale, and/or importing in the United States products, software, and/or services that incorporate or make use of one or more of the inventions covered by the '698 patent, including, but not limited to, systems, services, and/or software incorporating or implementing the Accused Products. SecureAuth thereby directly infringes one or more claims of the '698 patent, including at least claim 1 of the '698 patent. SecureAuth directly infringes at least through its own activities in making, using

(including through testing), selling, offering for sale, and/or importing the Accused Products as well as, to the extent applicable, jointly with activities of others under the direction and control of SecureAuth, including customers of SecureAuth and/or distributors who sell and offer to sell the Accused Products.

45. Upon information and belief, and as demonstrated by the allegations above and the supporting exhibits to this Complaint, the Accused Products satisfy each and every element of one or more claims of the ’698 patent, including, and without limitation, at least claim 1 of the ’698 patent.

46. For example, and without limitation, the Accused Products comprise a software method for employing a multichannel security system to control access to a computer (*e.g.*, software-based authentication platform of the SecureAuth Products). *See, e.g.*, Exhibit D at 1; Exhibit E at 1–5; Exhibit G at 1–2; Exhibit H at 1; Exhibit I at 1–2; Exhibit J at 7, 9; Exhibit K at 1–2; Exhibit L at 1–5; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 2–6, 8, 10–12; Exhibit P at 1–3, 5–7; Exhibit Q at 1–2. The Accused Products receive at an interception device in a first channel a login identification demand to access a host computer also in the first channel (*e.g.*, an element of the system that intercepts the user’s login request prior to granting access to the protected information in, for example, the computer or application). *See, e.g.*, Exhibit E at 1–5; Exhibit F at 2–3; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2; Exhibit N at 1–2; Exhibit O at 4–6, 8. The Accused Products verify the login identification (*e.g.*, by verifying the login information of the user). *See, e.g., id.* The Accused Products receive at a security computer in a second channel (*e.g.*, SecureAuth IdP Server or Cloud Access Server) the demand for access and the login identification and output a prompt requesting transmission of data (*e.g.*, push notification to user’s mobile device requesting user to accept or deny authorization and/or

select a symbol). *See, e.g.*, Exhibit E at 1–5; Exhibit F at 2–3; Exhibit H at 10; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 4–6, 8; Exhibit P at 7. The Accused Products receive the transmitted data at the security computer compare the transmitted data to predetermined data and depending on the comparison of the transmitted and the predetermined data, output an instruction from the security computer to the host computer to grant access to the host computer or deny access thereto (*e.g.*, SecureAuth IdP Server or Cloud Access Server receives the user's response and outputs an instruction to the protected computer to grant or deny access to the requested protected computer or application based on that response). *See, e.g.*, Exhibit E at 4; Exhibit G at 1–2; Exhibit H at 9; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 4–5; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 4–6, 8, 10–12; Exhibit P at 7.

47. Under 35 U.S.C. § 271(b), SecureAuth has indirectly infringed, and continues to indirectly infringe the '698 patent by, *inter alia*, inducing others to make, use, sell, offer for sale, and/or import into the United States the Accused Products. SecureAuth distributes, markets, and/or advertises the Accused Products in this District and elsewhere in the United States, including through at least SecureAuth's website and online demonstrations of its products. *See, e.g.*, Exhibits D–Q.

48. Upon information and belief, with knowledge of the '698 patent and its infringement thereof, SecureAuth distributes its marketing materials and advertisements, and provides support for installing and implementing the Accused Products, to knowingly instruct and direct users/customers to use the Accused Products in an infringing manner.

49. Under 35 U.S.C. § 271(c), with knowledge of the '698 patent and its infringement thereof, SecureAuth has indirectly infringed and continues to indirectly infringe the '698 patent

by, *inter alia*, knowingly providing to its customers the Accused Products, which constitute material components of an infringing out-of-band authentication system/service and that was especially made or adapted for use in that system, which are not staple articles or commodities of commerce and which have no substantial, non-infringing use. *See, e.g.*, Exhibit D at 1; Exhibit E at 1–5; Exhibit F at 1–26; Exhibit G at 1–2; Exhibit H at 1–13; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 1–5; Exhibit M at 1Exhibit N at 1–2; Exhibit O at 4–6, 8, 10–12; Exhibit P at 1–7.

50. SecureAuth puts the Accused Products into service and exercises control over said systems.

51. SecureAuth had and/or has knowledge of the ’698 patent and its infringement thereof at least as early as the filing of this Complaint.

52. SecureAuth’s customers directly infringe one or more claims of the ’698 patent by, for example, integrating the claimed systems and methods, including at least claim 1, directly into the customers’ web services and/or existing protected access control systems and directly benefitting from the use of those services and/or systems. For example, SecureAuth’s customers in the United States utilize the two-factor authentication systems and methods claimed in the ’698 patent, including at least claim 1, for the purpose of gaining secure access to, exemplarily, various Internet websites and other secure networks.

53. Upon information and belief, SecureAuth knowingly provides its customers with products and web services that are used in a manner that infringes one or more claims of the ’698 patent, including at least claim 1, as illustrated exemplarily above in paragraph 46.

54. Upon information and belief, through its marketing activities, instructions and directions, and through the sales and offers for sale of infringing systems and methods,

SecureAuth specifically intends for, and/or specifically encourages and instructs, its customers to use its products and web services and knows that its customers are using its products and web services in an infringing manner.

55. As a direct and proximate result of SecureAuth's acts of infringing one or more claims of the '698 patent, StrikeForce has suffered injury and monetary damages for which StrikeForce is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for SecureAuth's infringement.

56. SecureAuth will continue to directly infringe one or more claims of the '698 patent, causing immediate and irreparable harm to StrikeForce unless this Court enjoins and restrains SecureAuth's activities, specifically the acts of making, using, selling, and offering for sale, as previously outlined. There are inadequate remedies available at law to compensate for this harm.

57. Upon information and belief, SecureAuth's past and ongoing infringement of the '698 patent has been and continues to be with full knowledge of the '698 patent and SecureAuth's infringement thereof, at least as of the filing date of this Complaint. SecureAuth's knowing, willful, and deliberate infringement of one or more claims of the '698 patent, including at least claim 1, in conscious disregard of StrikeForce's rights makes this case exceptional within the meaning of 35 U.S.C. § 285 and justifies treble damages pursuant to 35 U.S.C. § 284.

COUNT III –INFRINGEMENT OF THE '701 PATENT

58. StrikeForce incorporates by reference the averments set forth in paragraphs 1 through 57.

59. Pursuant to 35 U.S.C. § 271(a), SecureAuth has directly infringed and continues to directly infringe the '701 patent by making, using, selling, offering for sale, and/or importing

in the United States products, software, and/or services that incorporate or make use of one or more of the inventions covered by the '701 patent, including, but not limited to, the Accused Products. SecureAuth thereby directly infringes one or more claims of the '701 patent, including at least claim 1 of the '701 patent. SecureAuth directly infringes at least through its own activities in making, using (including through testing), selling, offering for sale, and/or importing the Accused Products as well as, to the extent applicable, jointly with activities of others under the direction and control of SecureAuth, including customers of SecureAuth and/or distributors who sell and offer to sell the Accused Products.

60. Upon information and belief, and as demonstrated by the allegations above and the supporting exhibits to this Complaint, the Accused Products satisfy each and every element of one or more claims of the '701 patent, including, and without limitation, at least claim 1 of the '701 patent.

61. For example, and without limitation, the Accused Products comprise a security system for accessing a host computer (*e.g.*, software-based authentication platform of the SecureAuth Products). *See, e.g.*, Exhibit D at 1; Exhibit E at 1–5; Exhibit G at 1–2; Exhibit H at 1; Exhibit I at 1–2; Exhibit J at 7, 9; Exhibit K at 1–2; Exhibit L at 1–5; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 2–6, 8, 10–12; Exhibit P at 1–3, 5–7; Exhibit Q at 1–2. The Accused Products include an access channel comprising an interception device for receiving a login identification originating from an accessor for access to said host computer (*e.g.*, an element of the system that intercepts the user's login request prior to granting access to the protected information in, for example, the computer or application). *See, e.g.*, Exhibit E at 1–5; Exhibit F at 2–3; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2; Exhibit N at 1–2; Exhibit O at 4–6, 8. The Accused Products include, in an authentication channel, a security computer

(*e.g.*, *e.g.*, SecureAuth IdP Server or Cloud Access Server) for receiving from said interception device said login identification and for communicating access information to said host computer and for communicating with a peripheral device of said accessor (*e.g.*, push notification to user's mobile device requesting user to accept or deny authorization and/or select a symbol). *See, e.g.*, Exhibit E at 4-5; Exhibit F at 1; Exhibit G at 1–2; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2; Exhibit N at 1–2; Exhibit O at 4–6, 8; Exhibit P at 6–7. The Accused Products include a database having at least one peripheral address record corresponding to said login identification (*e.g.*, database accessed by SecureAuth IdP Server or Cloud Access Server for communicating with the user's mobile device). *See, e.g.*, Exhibit H at 2–3 (explaining how a user enrolls the SecureAuth Authenticate mobile app into the SecureAuth IdP system); *see also, e.g.*, Exhibit I at 2; Exhibit L at 1–2; Exhibit N at 1–2; Exhibit O at 4–6. The Accused Products include, in an authentication channel, a prompt mechanism for instructing said accessor to enter predetermined data at and transmit said predetermined data from said peripheral device (*e.g.*, an element of the system that issues a push notification on the user's mobile device prompting the user to accept or deny authorization and/or select a symbol). *See, e.g.*, Exhibit F at 22–23; Exhibit G at 1–2; Exhibit H at 9–11; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 2, 4; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 4–6, 8; Exhibit P at 7. The Accused Products include, in an authentication channel, a comparator for authenticating access demands in response to the transmission of said predetermined data by verifying a match between said predetermined data and said entered and transmitted data, wherein said security computer outputs an instruction to the host computer to either grant access thereto using said access channel or to deny access thereto (*e.g.*, SecureAuth IdP Server or Cloud Access Server receives the user's response and outputs an instruction to the protected computer to grant or deny access

to the requested protected computer or application based on that response). *See, e.g.*, Exhibit E at 4; Exhibit G at 1–2; Exhibit H at 9; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 4–5; Exhibit M at 1; Exhibit N at 1–2; Exhibit O at 4–6, 8, 10–12; Exhibit P at 7.

62. Under 35 U.S.C. § 271(b), SecureAuth has indirectly infringed and continues to indirectly infringe the '701 patent by, *inter alia*, inducing others to make, use, sell, offer for sale, and/or import into the United States the Accused Products. SecureAuth distributes, markets, and/or advertises the Accused Products in this District and elsewhere in the United States, including through at least SecureAuth's website and online demonstrations of its products. *See, e.g.*, Exhibits D–Q.

63. Upon information and belief, with knowledge of the '701 patent and its infringement thereof, SecureAuth distributes its marketing materials and advertisements, and provides support for installing and implementing the Accused Products, to knowingly instruct and direct users/customers to use the Accused Products in an infringing manner.

64. Under 35 U.S.C. § 271(c), with knowledge of the '701 patent and its infringement thereof, SecureAuth has indirectly infringed, and continues to indirectly infringe the '701 patent by, *inter alia*, knowingly providing to its customers the Accused Products, which constitute material components of an infringing out-of-band authentication system/service and that was especially made or adapted for use in that system, which are not staple articles or commodities of commerce and which have no substantial, non-infringing use. *See, e.g.*, Exhibit D at 1; Exhibit E at 1–5; Exhibit F at 1–26; Exhibit G at 1–2; Exhibit H at 1–13; Exhibit I at 1–2; Exhibit J at 9; Exhibit K at 1–2; Exhibit L at 1–5; Exhibit M at 1Exhibit N at 1–2; Exhibit O at 4–6, 8, 10–12; Exhibit P at 1–7.

65. SecureAuth puts the Accused Products into service and exercises control over said systems.

66. SecureAuth had and/or has knowledge of the ’701 patent and its infringement thereof, at least as early as the filing of this Complaint.

67. SecureAuth’s customers directly infringe one or more claims of the ’701 patent by, for example, integrating the claimed systems and methods, including at least claim 1, directly into the customers’ web services and/or existing protected access control systems and directly benefitting from the use of those services and/or systems. For example, SecureAuth’s customers in the United States utilize the two-factor authentication systems and methods claimed in the ’701 patent, including at least claim 1, for the purpose of gaining secure access to, exemplarily, various Internet websites and other secure networks.

68. Upon information and belief, SecureAuth knowingly provides its customers with products and web services that are used in a manner that infringes one or more claims of the ’701 patent, including at least claim 1, as illustrated exemplarily above in paragraph 61.

69. Upon information and belief, through its marketing activities, instructions and directions, and through the sales and offers for sale of infringing systems and methods, SecureAuth specifically intends for, and/or specifically encourages and instructs, its customers to use its products and web services and knows that its customers are using its products and web services in an infringing manner.

70. As a direct and proximate result of SecureAuth’s acts of infringing one or more claims of the ’701 patent, StrikeForce has suffered injury and monetary damages for which StrikeForce is entitled to relief in the form of damages for lost profits and in no event less than a reasonable royalty to compensate for SecureAuth’s infringement.

71. SecureAuth will continue to directly infringe one or more claims of the '701 patent, causing immediate and irreparable harm to StrikeForce unless this Court enjoins and restrains SecureAuth's activities, specifically the acts of making, using, selling, and offering for sale, as previously outlined. There are inadequate remedies available at law to compensate for this harm.

72. Upon information and belief, SecureAuth's past and ongoing infringement of the '701 patent has been and continues to be with full knowledge of the '701 patent and SecureAuth's infringement thereof, at least as of the filing date of this Complaint. SecureAuth's knowing, willful, and deliberate infringement of one or more claims of the '701 patent, including at least claim 1, in conscious disregard of StrikeForce's rights makes this case exceptional within the meaning of 35 U.S.C. § 285 and justifies treble damages pursuant to 35 U.S.C. § 284.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against SecureAuth as follows:

A. Declaring that the '599 patent was duly and legally issued, and is valid and enforceable;

B. Declaring that the '698 patent was duly and legally issued, and is valid and enforceable;

C. Declaring that the '701 patent was duly and legally issued, and is valid and enforceable;

D. Declaring that SecureAuth has infringed the '599 patent;

E. Declaring that SecureAuth has willfully infringed the '599 patent;

F. Declaring that SecureAuth has infringed the '698 patent;

G. Declaring that SecureAuth has willfully infringed the '698 patent;

H. Declaring that SecureAuth has infringed the ’701 patent;

I. Declaring that SecureAuth has willfully infringed the ’701 patent;

J. Awarding to Plaintiff damages caused by SecureAuth’s infringement, including all lost profits resulting from SecureAuth’s acts of infringement, and in no event less than reasonable royalties, together with pre-judgment and post-judgment interest and supplemental damages for any continuing post-verdict infringement up until entry of the final judgment, with an accounting, as needed, pursuant to 35 U.S.C. § 284;

K. Awarding to Plaintiff treble damages for infringement of the ’599, ’698, and ’701 patents as a consequence of SecureAuth’s willful infringement;

L. Enjoining SecureAuth, its officers, agents, servants, employees, attorneys, all parent and subsidiary corporations and affiliates, its assigns and successors in interest, and those persons in active concert or participation with SecureAuth who receive notice of the injunction, from continuing acts of infringement of the ’599, ’698, and ’701 patents;

M. Ordering that, in the event a permanent injunction preventing future acts of infringement is not granted, Plaintiff be awarded a compulsory ongoing license fee;

N. Adjudging this an exceptional case and awarding to Plaintiff its reasonable attorneys fees pursuant to 35 U.S.C. § 285; and

O. Awarding to Plaintiff such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to Rule 38(b), Fed. R. Civ. P., Plaintiff demands a trial by jury on all of the claims so triable.

Dated: March 16, 2017

Respectfully submitted,

By: */s/ Stephen E. Noona*

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
senoona@kaufcan.com
Telephone: (757) 624-3239
Facsimile: (888) 360-9092

Richard T. McCaulley, Jr. (*pro hac vice to be filed*)
ROPES & GRAY LLP
191 North Wacker Drive
32nd Floor
Chicago, IL 60606
Telephone: (312) 845-1200

Steven Pepe (*pro hac vice to be filed*)
Kevin J. Post (*pro hac vice to be filed*)
ROPES & GRAY LLP
1211 Avenue of the Americas
New York, NY 10036-8704
Telephone: (212) 596-9000

Matthew J. Rizzolo (*pro hac vice to be filed*)
ROPES & GRAY LLP
2099 Pennsylvania Ave, NW
Washington, DC 20006
Telephone: (202) 508-4600

Attorneys for Plaintiff StrikeForce Technologies, Inc.